EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Michael A. Cofield (applicants' representative), Registration No. 54,630 on 07/17/2008.

The application has been amended as follows:

Claims 1-53 are cancelled.

54. (Currently Amended) A method, comprising:

determining at a local server whether a user is authorized to access a remote server;

when the user is authorized, identifying at the local server a first privilege level associated with the user, the identified first privilege level defining how the user is permitted to control an Operating System (OS) installed on the remote server;

logging the local server onto the OS, the logon using a generic account that provides the local server a second different privilege level for accessing the OS on the remote server, the generic account being non-corresponding with the identified first privilege level, wherein the generic account does not restrict privileges according to the identified first privilege level and the local server imposes administrative privilege level restrictions on the user, and the generic account allows multiple users access to the remote server through a single account logon ~~said login using a first account that gives the local server unrestricted administrative access to the OS installed on the remote server, said unrestricted login being non-corresponding with the identified privilege level~~;

receiving at the local server one or more commands entered ~~from the user~~ through a web browser associated with the user, wherein the commands are configured to allow the user to administer the remote server through the web browser without requiring direct access to the remote server, and wherein the commands are configured to establish, run and manage files on the OS ~~the commands for controlling the OS~~;

filtering the commands received at the local server according to a verification of whether the received commands correspond to the identified first privilege level for the user; ~~and~~

sending messages that represent the filtered commands from the local server, over a packet switched network, and to the remote server when the filtered commands correspond to the identified first privilege level;

wherein at least one of the received commands is blocked through the filtering by the local server, the blocked command being one that is permissible under the second privilege level ~~with unrestricted administrative access~~ such that said filtering and sending by the local server simulates user OS logon using a user ~~second different~~ account having the identified first privilege level ~~restricted administrative privileges to~~

~~the OS installed on the remote server~~ while the local server is actually logged onto, and accessing, the remote server using the generic ~~first~~ account having the second privilege level ~~unrestricted administrative privileges~~[[.]]; and

creating a session log identifying the commands represented by the messages, the session log containing information to allow a system administrator to undo transactions performed on the OS, wherein the transactions alter a file system stored on the remote server and the session log contains information to allow the system administrator to rebuild the file system.

55. (Previously presented) The method of claim 54 wherein said logon is conducted using an operating system level account that is selected independently of the user.

56. (Previously Presented) The method of claim 54 wherein the messages are sent using a transfer protocol that operates independently of HyperText Transfer Protocol (HTTP) capability on the remote server and that operates independently of TELecommunications NETwork (TELNET) capability on the remote server.

57. (Cancelled)

58. (Currently amended) The method of claim 54 wherein the messages are configured to cause the remote server to download files to a client system separate from the remote server.

59. (Previously Presented) The method of claim 58 wherein the client system is a same client system that originates the commands.

60-61. (Cancelled)

62. (Currently Amended) A local server ~~A system~~, comprising:

one or more processors; and

a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

determine whether a user is authorized to access a remote server;

when the user is authorized, identify a first privilege level associated with the user, the identified first privilege level defining how the user is permitted to control an Operating System (OS) installed on the remote server;

log the local server onto the OS, the logon using a generic account that provides the local server a second different privilege level for accessing the OS on the remote server, the generic account being non-corresponding with the identified first privilege level, wherein the generic account does not restrict privileges according to the identified first privilege level and the local server is configured to impose administrative privilege level restrictions on the user, and the generic account allows multiple users access to the remote server through a single account logon;

receive one or more commands entered through a web browser associated with the user, wherein the commands are configured to allow the user to administer the remote server through the web browser without requiring direct access to the remote server, and wherein the commands are configured to establish, run and manage files on the OS;

filter the received commands according to a verification of whether the received commands correspond to the identified first privilege level for the user;

send messages that represent the filtered commands from the local server, over a packet switched network, and to the remote server when the filtered commands correspond to the identified first privilege level;

wherein at least one of the received commands is blocked through the filtering by the local server, the blocked command being one that is permissible under the second privilege level such that said filtering and sending by the local server simulates user OS logon using a user account having the identified first privilege level while the local server is actually logged onto, and accessing, the remote server using the generic account having the second privilege level; and

create a session log identifying the commands represented by the messages, the session log containing information to allow a system administrator to undo transactions performed on the OS, wherein the transactions alter a file system stored on the remote server and the session log contains information to allow the system administrator to rebuild the file system.

~~a content server having configured thereon an Operating System (OS) , the OS capable of provisioning different OS logon accounts that define different levels of administrative privileges for different users;~~

~~the content server having established thereon an OS logon account configured to allow a first range of administrative privileges to a logged on user;~~

~~one or more central servers to function as a trusted proxy for the content server by remotely administering privilege management for the content sever, the central servers to log onto the OS using the established OS logon account that provides the first range of administrative privileges;~~

~~the central servers to receive an access request from one of the remote users, to determine whether the remote user is authorized to access the content server, and when the remote user is authorized to access the content server, to select a level of administrative privileges according to the remote user; and~~

~~the central servers to receive, from an endpoint for the remote user, commands for controlling the content server, to filter the received commands according to the selected level of administrative privileges such that the user can be restricted to a second range of administrative privileges, the second range being a subset of the first range of administrative privileges, and to forward the filtered commands to the content server while the central server is logged onto the content server using the OS logon account having the first range of administrative privileges.~~

63. (Cancelled)

64. (Currently Amended) The local server ~~system~~ of claim 62 wherein the local server is configured to remain ~~central servers are~~ logged onto the remote ~~content~~ server under the generic ~~OS logon~~ account when forwarding the filtered commands for other users ~~the different users~~.

65. (Currently Amended) The local server ~~system~~ of claim 62 wherein the commands ~~are generated by the remote user interacting with a web browser and~~ are formatted as HyperText Transfer Protocol (HTTP) requests, and the local server is configured to send the messages ~~forwards the commands~~ using an File Transfer Protocol (FTP) format.

66. (Currently Amended) The local server ~~system~~ of claim 62, wherein the processors are further operable to ~~further comprising~~:

~~the central server to~~ send a notification to the ~~remote~~ user when one of the commands is filtered, the notification indicating that the ~~remote~~ user does not have a requisite level of administrative privileges to control the remote ~~content~~ server using the filtered command.

67-68. (Cancelled)

69. (Currently Amended) The local server ~~system~~ of claim 62 wherein the received commands are for creating files and directories, editing files and directories, or removing files and directories.

70. (Currently Amended) The local server ~~system~~ of claim 62 wherein a file structure on the remote ~~content~~ server is manipulated according to the messages ~~forwarded commands~~.

71. (Currently Amended) The local server ~~system~~ of claim 62 wherein the OS is an embedded OS.

72-79. (Cancelled)

REASONS FOR ALLOWANCE

1. Claims 54-56, 58-59, 62, 64-66 and 69-71 are allowed.

2. The following is a statement of reasons for the indication of allowable subject matter:

In interpreting the claims in light of the specification and applicant's arguments, the Examiner finds the claimed invention is patentably distinct from the prior art of record.

The prior art of record includes Devine et al. (Devine), US Patent No. 6,606,708, Riggins, US Patent No. 7,287,271, Booth, US Patent No. 6,345,307, Lomet et al. (Lomet), US Patent No. 6,182,086, and Brown et al. (Brown), US Patent No. 5,941,947.

Devine discloses a dispatcher server (local server) authenticates the user's access to the desired middle-tier service from mid-range server (remote server) (col. 13, line 60 – col. 14, line 5). Devine further discloses providing for an identification of the user, and an identification of the user is who he/she claims to be and a determination of entitlements that the user may avail themselves of within the enterprise system (Abstract); and the entitlements represent specific services the user has subscribed and has privilege to access (col. 16, lines 44-54). Devine further discloses : the user is able to select a service or a request to run, and the service can be a command and control, read, write and modify files (col. 16, lines 60-66 and col. 27, lines 2-9). Devine further discloses the dispatcher receiving the requests from the user, the request then is examined, revealing the user and the target middle-tier service for the request, and performing validation, making sure that the user is entitle to communicate with the desired service, and managing the communication of the specific customer request with the middle-tier server to actually get the request serviced (col. 14, lines 6-32).

Riggins discloses the user must first obtain authorization from the global server (local server), and once authenticated, the global server 106 provides the user with access to the services, and varying levels of access to services will be granted based on varying strengths of identification and authentication (col. 4, lines 24-34).

Booth discloses a proxy server is a type of gateway that allows a browser using HTTP to communicate with a server that does not understand HTTP, but which uses FTP; the proxy server accepts HTTP requests from the browser and translates them into a format that is suitable for the origin server such as an FTP request (col. 1, lines 34-45), and thus this implies the requests are sent using a transfer protocol FTP that operates independently of HyperText Transfer Protocol (HTTP) capability on the remote server and that operates independently of TELecommunications NETwork (TELNET) capability on the remote server.

Lomet discloses server 54 generates a log record for each of its own write operation on database objects (col. 10, lines 35-41). Lomet further discloses the server can undo a request and re-execute it all over again when the client re-submits the request (col. 10, line 59 - col. 11, line 2). Lomet further discloses when restarting after a server failure, the server performs analysis pass over log file by rebuilding the active application table (file system) (col. 15, line 60 - col. 16, line 12).

Brown discloses access rights data is stored within the relational database association with multiple user group identifiers, which identify user groups (col. 3, lines 12-20). Brown further discloses upon receiving a user-specific access rights query, the security server (content server) accesses the group-member table to identify all user groups of which the specified user is a member (col. 4, lines 40-65).

3. Claim 54 is allowed because the prior art of record does not expressly disclose alone or in combination the logon the local server onto the operating system (OS) using a generic account that provides the local server a second different privilege level for accessing the OS on the remote server, the generic account being non-corresponding with the identified first privilege level, wherein the generic account does not restrict privileges according to the identified first privilege level and the local server imposes administrative privilege level restrictions on the user, and the generic account allows multiple users access to the remote server through a single account logon; receiving at the local server one or more commands entered through a web browser associated with the user, wherein the commands are configured to allow the user to administer the remote server through the web browser without requiring direct access to the remote server, and wherein the commands are configured to establish, run and manage files on the OS; and wherein at least one of the received commands is blocked through the filtering by the local server, the blocked command being one that is permissible under the second privilege level such that said filtering and sending by the local server simulates user OS logon using a user account having the identified first privilege level

while the local server is actually logged onto, and accessing, the remote server using the generic account having the second privilege level.

4. Claims 55-56 and 58-59 further limit independent claim 54. Claims 62, 64-66 and 69-71 are allowed as well for the same reason set forth for claims 54-56 and 58-59.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the Issue Fee and, to avoid processing delays, should preferably accompany the Issue Fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Drawings

6. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings submitted on 10/18/1999 are informal. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chau Nguyen whose telephone number is (571) 272-4092. The Examiner can normally be reached on Monday-Friday from 8:30 am to 5:30 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Doug Hutton, can be reached at (571) 272-4137.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. On July 15, 2005, the Central Facsimile (FAX) Number will change from 703-872-9306 to 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chau Nguyen
Patent Examiner
Art Unit 2176

/Rachna S Desai/
Primary Examiner, Art Unit 2176